

UNCLASSIFIED//FOR OFFICIAL USE ONLY



CALIFORNIA STATE THREAT ASSESSMENT CENTER

24-HOUR REPORT

21 DECEMBER 2018

(U) CALIFORNIA

(U) Santa Ana – Five California Deputies Attacked, Injured By Jail Inmates

(U) Five deputies at a California correctional facility were hospitalized after they were attacked by inmates on Thursday morning. The attacks happened around 7:30 a.m. as inmates were exchanging items in a hallway at the Central Men's Jail in Santa Ana, according to the Orange County Sheriff's Office. The jail was placed on a temporary lockdown following the incident, which officials said was "quickly controlled." Officials said that five deputies and one inmate were transported to the hospital with moderate injuries. Several other inmates who were involved were examined and returned to their jail cells.

SOURCE: 20 December 2018, [Fox News](#)

(U) SOUTHWEST BORDER

(U) District of Columbia – US Sending Migrants Back to Mexico to Wait Out Asylum Requests

(U) Washington – The United States will soon send non-Mexican migrants who cross the US southern border back to wait in Mexico while their US asylum requests are processed, a major change in immigration policy, according to the Trump administration. Immigrant advocates and human rights experts quickly denounced the policy change as illegal and violating the rights of refugees. Mexico's government said that it would accept some of those migrants for humanitarian reasons.

SOURCE: 20 December 2018, [Reuters](#)

(U) NATIONAL

(U) District of Columbia – US Charges Two with China Intelligence Ties in Hacking Case

(U) Washington – US officials say two Chinese citizens acting on behalf of their country's main intelligence agency carried out an extensive hacking campaign to steal data from military service members, government agencies and private companies in the United States and nearly a dozen other nations. It was the latest in a series of Justice Department indictments targeting cyberespionage from Beijing. The two are accused of breaching computer networks in a broad swath of industries, including aviation and space, banking and finance, oil and gas exploration and pharmaceutical technology.

SOURCE: 20 December 2018, [AP](#)

(U) Washington – Microsoft Issues Emergency Update to Fix Critical Flaw

(U) Seattle – Microsoft has issued an emergency update that fixes a critical Internet Explorer vulnerability that attackers are actively exploiting on the Internet. The memory-corruption flaw allows attackers to remotely execute malicious code when computers use IE to visit a booby-trapped website, Microsoft said Wednesday. Indexed as CVE-2018-8653, the flaw affects all supported versions of Windows. The vulnerability involves the way Microsoft's scripting engine handles objects in memory in Internet Explorer. In a separate advisory, Microsoft said the vulnerability is being used in targeted attacks, but the company didn't elaborate.

SOURCE: 20 December 2018, [Ars Technica](#)

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Form # 1168-442e-b407-de1a8c242c14

UNCLASSIFIED//FOR OFFICIAL USE ONLY**(U) INTERNATIONAL****(U) Albania – Iranian Diplomats Expelled from Country Plotted Against Dissidents**

(U) Tirana – Two Iranian diplomats recently expelled from the Balkan nation of Albania were tied to an alleged plot to attack an exiled group inside the country earlier this year, according to sources. Albanian authorities expelled Iran's ambassador to the country and another diplomat, accusing the two of "violating their diplomatic status," amid an ongoing regional intelligence and diplomatic battle between Iran versus the US and its partners. Two alleged Iranian members of the Revolutionary Guard's Quds Force, its foreign secret operations branch, were caught planning "an explosive" attack against the base or personnel of the Mujahedin-e-Khalq, or MEK.

SOURCE: 20 December 2018, [The Independent](#)

(U) China – Hackers Target HPE, IBM and Clients

(U) Beijing – Hackers working on behalf of China's Ministry of State Security breached the networks of Hewlett Packard Enterprise Co and IBM, then used the access to hack into their clients' computers, according to sources familiar with the attacks. The attacks were part of a Chinese campaign known as Cloudhopper, which the United States and Britain on Thursday said infected technology service providers in order to steal secrets from their clients. While cybersecurity firms and government agencies have issued multiple warnings about the Cloudhopper threat since 2017, they have not disclosed the identity of technology companies whose networks were compromised.

SOURCE: 20 December 2018, [Reuters](#)

(U) Germany – Airports on Alert Amid Spying Reports at Stuttgart

(U) Stuttgart – Germany's biggest airports are on alert after four suspected terrorists were spotted staking out Stuttgart airport, according to reports. Police are said to be hunting for a father and son from North Rhine-Westphalia and two others seen taking photos of the airport's terminal and grounds. Details of the suspects were passed to German police by Morocco's secret service, according to reports. This comes one week after a Christmas market terror attack across the border in France.

SOURCE: 20 December 2018, [BBC](#)

(U) PREPARED BY THE CALIFORNIA STATE THREAT ASSESSMENT CENTER.

(U) FOR QUESTIONS OR CONCERNS, PLEASE EMAIL STAC@CALOES.CA.GOV, OR CALL 916-636-2900.

Warning: This document is the exclusive property of the State Threat Assessment Center (STAC) and is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the California Public Records Act (Govt. Code Sec. 6250-6270). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with STAC policy relating to U//FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid "need-to-know" without prior approval of an authorized STAC official. No portion of this report should be furnished to the media, either in written or verbal form.

This document contains excerpts of suspicious activities and incidents of interest to the STAC as obtained from open and unclassified sources.